

first access to the intelligent interconnecting device from outside has occurred;

a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on

the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred;

a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given;

a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given;

a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the

external apparatus is judged to be the first access
in said fourth step;

5 a sixth step of determining the external
apparatus as an apparatus not to be responded to
thereafter by the intelligent interconnecting
device when the external apparatus is judged not
to be authenticated in said third step;

10 a seventh step of causing the intelligent
interconnecting device to judge whether or not the
source IP address of the external apparatus giving
the access thereto is identical with the stored
source IP address when this access is judged not
to be the first access in said first step;

15 an eighth step of causing the intelligent
interconnecting device to judge whether or not the
source IP address is within a predetermined valid
period when the source IP address of the external
apparatus is judged to be identical with the stored
source IP address in said seventh step;

20 a ninth step of determining the external
apparatus having the source IP address which is
judged to be within the predetermined valid period
as an apparatus to be responded to thereafter by
the intelligent interconnecting device and causing
25 the intelligent interconnecting device to execute

the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step; and

5 a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent
10 interconnecting device, when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step.

15 8. An unauthorized access avoiding program which is executed in an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality
20 of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, the unauthorized access avoiding program for an intelligent interconnecting device comprising:

25 a first step of causing the intelligent